

TOP SECRET//COMINT//NOFORN NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE

FORT GEORGE G. MEADE, MARYLAND 20755-6000

02 March 2010

MEMORANDUM FOR THE ASSISTANT TO THE SECRETARY OF DEFENSE (INTELLIGENCE OVERSIGHT)

SUBJECT: (U//FOUO) Required Actions for the CY 2009 Intelligence Oversight Report to Congress – INFORMATION MEMORANDUM

(U//FOUO) In accordance with your memorandum of 21 October 2009, the enclosed consolidation of the National Security Agency's Quarterly Reports to the President's Intelligence Oversight Board for calendar year 2009 is provided to assist the Secretary of Defense in preparation of his Annual Report to Congress.

Meange Elland
GEORGE ELLARD
Inspector General

Encl:
Annual Report

This document may be declassified and marked "UNCLASSIFIED//FOR OFFICIAL USE ONLY" upon removal of enclosure(s).

Approved for Release by NSA on 12-19-2014, FOIA Case # 70809 (Litigation)

TOP SECRET//COMINT//NOFORN-

1. (U//FOUO) Intelligence, counterintelligence, and intelligence-related activities that violate law, regulation, or policy substantiated during the year, as well as actions taken as a result of the violations

(b)	1) 3)-P.L. 86-36 (U) Intelligence Activities
	(U) Unintentional Collection against United States Persons or Persons in the United States
	instances in which Signals Intelligence (SIGINT) analysts inadvertently collected communications to, from, or about United States (U.S.) persons while pursuing foreign intelligence tasking were reported in CY 2009. Those instances of unintentional collection were caused by tasking selectors (e.g., telephone numbers) thought to be foreign that were discovered to be in the United States, delays in detasking, procedural errors, software-related problems, typographical errors, one case in which Communications Security (COMSEC) monitoring data was inappropriately reviewed, and other human error. Intercepts and reports have been deleted or destroyed where required by United States SIGINT Directive (USSID) SP0018.
	(TS//SI//REL TO USA, FVEY) During this reporting period, valid foreign intelligence targets the United States. Collection on those targets occurred due to detasking delays, software-related problems, procedural errors, and human error.
	(U) Tasking Error (b)(1) (b)(3)-P.L. 86-36
	(TS//SI//REL TO USA, FVEY) A U.S. telephone number was mistakenly tasked for collection. an NSA analyst tasked a telephone number believed to be associated with a foreign intelligence target. The selector was detasked on and one resulting intercept was deleted. No reports were issued on the collection.
	(TS//SI//RFL TO USA, FVEY) an NSA learned th(b)(3)-50 USC 3024(tasked telephone number selectors believed to be used by foreign intelligence targets The resulting collection of calls was deleted and the selectors were detasked on No reporting was produced based on the collection.
	(U) One End of the Communication in the United States
	(b)(1) (b)(3)-P.L. 86-36 unminimized SIGINT
	(b)(1) (L. 86-36 (b)(3)-P.L. 86-36 (b)(3)-18 USC 798 (b)(3)-50 USC 3024(i) Derived From: NSA/CSSM 1-52 Dated: 20070108 Declassify On: 20320108

TOP SECRET//COMINT//NOFORN

(b)(1) (b)(3)-P.L. 86-36 (b)(3)-18 USC 798 (b)(3)-50 USC 3024(i)

(U) Poorly Constructed Database Queries
(TS//SI//NF) On occasions, NSA analysts employed poorly constructed database queries, and on of those occasions, the queries returned results from the database. Problems were caused by analysts querying selectors thought to be foreign but were discovered to be in the United States, misunderstandings of authority, overly broad search terms, procedural errors such as failure to confirm the location of targets, software-related problems, other human error, and one case in which COMSEC selectors were used in a SIGINT database. The returned results from the overly broad or incomplete queries were deleted, and no reports were issued. NSA counseled or retrained analysts who misunderstood NSA authorities.
(U) Detasking Delays (b)(1) (b)(3)-P.L. 86-36
(U// FOUO) On occasions, NSA analysts failed to remove selectors from tasking due to human and procedural errors.
(U//F OUO) Dissemination of U.S. Identities
TS//SI//REL TO USA, FVEY) The NSA enterprise issued approximately SIGINT product reports during 2009. In those reports, there were instances in which SIGINT analysts disseminated communications to, from, or about U.S. persons while pursuing foreign intelligence. A total of SIGINT products were cancelled as NSA analysts learned of the U.S. persons, organizations, or entities named in the products without authorization. The data was deleted or destroyed when required and the reports were not reissued or they were reissued with proper minimization.
(U) Report Cancellation Delay (b)(1) (b)(3)-P.L. 86-36
an NSA analyst learned from that a valid foreign target held dual and U.S. citizenship. Although the selectors were detasked on and collection was purged from NSA databases, reports generated from the unauthorized collection were not cancelled until. The delay in report cancellation occurred because of a miscommunication between two analysts. Each believed the other was going to cancel the reports.
a SIGINT analyst forwarded an e-mail containing a U.S. identity without considering USSID SP0018 implications. The e-mail was recalled, and the customer was asked to destroy copies of the information.
(U) Foreign Intelligence Surveillance Act (FISA) Activities
(TS//SI//NF) NSA incurred violations related to Foreign Intelligence Surveillance Court (FISC)-authorized targets in 2009. There were instances in which selectors were detasked
(b)(1) (b)(3)-P.L. 86-36 TOP SECRET//COMINT//NOFORN

	late, in which tasking occurred before authorization, in which selectors
	instances of misunderstanding the authority, in which FISC-
	approved selectors were misused, from an unapproved selector, and from other human
	error. There was also one case of improper dissemination.
	(b)(1)
	(U) Retention (b)(3)-P.L. 86-36
	(S//REL TO USA, FVEY) an NSA database developer noted that a database
	contained FISA data older than the retention time authorized by the Court. All files containing
	the FISA data were moved To prevent future retention errors, the
	developers implemented a process containing FISA data.
	containing 1 15A data.
	(TS//SI/NF)
	-P.L. 86-36
	-18 USC 798
	-50 USC 3024(i)
_	(TS//SI//NF) Business Records FISA (BR FISA)
	- (LINE INTERPRETATION (BITTION)
-	(TS//SI//NF) There were two violations of the BR FISC Order, one due to lack of Reasonable
	Articulable Suspicion (RAS) and one for exceeding call chaining guidelines. No data was
	retained, and no reports were issued. Additionally, an NSA analyst forwarded reports to
	personnel who did not have required BR Order training.
	personner who did not have required BR Order training.
	(TS//SI//NF) the Department of Justice reported to the FISC that the
	(TS//SI//NF) the Department of Justice reported to the FISC that the NSA had been using an "alert list" to compare incoming BR FISA metadata against
	telephone numbers associated with counterterroriem (CT) towards that the NGA 1-1-1-1
	telephone numbers associated with counterterrorism (CT) targets that the NSA had tasked for SIGINT collection. The alert list contained numbers that NSA determined that a RAS
	evicted and that the numbers were related to a terrorist constitution of the state
	existed and that the numbers were related to a terrorist organization associated with However, the majority of selectors on the elect list had (b)(3)-P.L. 86-36
	The wever, the majority of selectors on the afert list had
	not been subjected to a RAS determination. Analysis through call-chaining was not
	performed unless the number met the RAS standard.
	(TS//SI/NF) the NSA suspended the comparison of BR FISA metadata
-	, and the state of
	against CT target selectors, and during a comprehensive review, the NSA identified other
	processes used to query the BR FISA metadata that also did not conform with the Court's
	orders or that were not fully explained to the Court. The review also identified some
	manually entered queries that were noncompliant with the Court's orders. None of the
	compliance incidents resulted in the dissemination of any reporting from the NSA to any
	other department or agency. Upon discovery of these compliance incidents, the NSA
	immediately made changes to its processes to ensure that handling and querying of the
	telephony metadata was in accordance with the Court's orders. The corrective measures
	included implementation of controls to prevent any automated querying of the telephony
	· · · · · · · · · · · · · · · ·

TOP SECRET//COMINT//NOFORN

metadata NSA receives pursuant to the Court's orders and to guard against manual querying errors.

(TS//SI/NF) The Department of Justice filed preliminary notices of compliance incidents with the FISC on 15 January, 21 January, 26 January, 2 February, 25 February, and 31 March 2009. The FISC issued an order on 5 March 2009 that allowed NSA to continue to acquire the BR FISA metadata but imposed further restrictions on use of the data.

(TS//SI/NF) On 24 June 2009, during the end-to-end review of the FISA BR Order

		t, containing U.S. information,	(b)(1)
	purged the	data from its repositories on 24 J	une (b)(3)-F
2009.		* 1	
		(b)(
(TS//SI//NF) Pen Register	/Trap and Trace Order (3)-P.L. 86-36 3)-50 USC 30
(TO JOY INTEX TO	that the contract of the contract of		
	violations of the PR/TT Or	der due to an analyst using an ear	
version of a software tool		and a new software tool	hat
(TS//SI//NF) In Court Order	PR/TT and previous	orders, the FISC authorized the	
installation and use of pen re	gisters and tran and trace de	vices as described in the government	ent's
		fy the sources or destinations of	icht s
specified electronic commun		NSA's	Office
of General Counsel learned the			
	fically authorized by the Ord		7 '
informed the Department of .	Justice's National Security I	Division that, in consultation with	the
Director, NSA/Chief, CSS, it	had instructed NSA analyst	s to cease querying the PR/TT m	etadata
until the matter was resolved	and with the Court's expres	s approval to resume receipt of	
specified communications an	d to resume its previous ope	erational practices. The Order exp	oired
	in NSA's possession was q	uarantined and collection ceased.	
86-36 -(TS//SI//NF) The Protect A	America Act of 2007 (PA	A) There were PAA inciden	te in
2009 due to tasking selectors	thought to be foreign but di	scovered to be in the United State	es.
delays in detasking, tasking s	selectors under the wrong ce	rtification, and a typographical en	ror.
(U) The FISA Amendmen	its Act (FAA)	√	
		(b)(1) (b)(3)-P.L. 86-36	
(U) Section 702		(D)(3)-P.L. 80-30	
ABOUGE (NE) TO	A surface and the surface and	<u> </u>	
(15//51//Pi) There were	violations of FAA Section 7	02 authority due to tasking under	the
wrong FAA certification,	violations due to tasking s	electors thought to be foreign but	
discovered to be in the Unite	d States,violations due to	o detasking delays, violations	due to
software errors, violation	is where no reasonable artic	ulable suspicion was found, one	

TOP SECRET//COMINT//NOFORN

violation due to collection at an unapproved location, one violation due to procedural error, and one violation for tasking prior to approval.

(U) Dissemination of FAA Data
(TS//SI/NF) unminimized collection containing a U.S. selector was forwarded to in an analyst-to-analyst exchange. When the violation was identified, the message was successfully recalled
(U// FOUO) an NSA analyst forwarded FAA data to NSA personnel, some of whom were not authorized to view FAA data. The e-mail was recalled and recipients deleted copies on (b)(1) (b)(3)-P.L. 86-36
(U// FOUO) an NSA analyst forwarded an e-mail containing FAA data to recipients, three of whom had not completed training required for access to FAA information. Within one hour of recognizing the mistake, the three analysts not authorized access to FAA data had deleted the e-mail.
(TS//SI/NF) On occasions in November 2009, NSA analysts forwarded unminimized FAA SIGINT on targets tasked under FAA customer not authorized to view unminimized FAA SIGINT. In the instances, e-mail selectors associated with U.S. entities or persons were left unminimized in SIGINT reporting. All reports were either revised or reissued with proper minimization.
(U) Destruction Delay (b)(3)-P.L. 86-36 (b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i)
(TS//SI/NF) U.S. person data was retained before an NSA analyst purged it from NSA databases. The target, believed to be foreign at the time of tasking on was found to be a U.S. citizen in The analyst intended to request authorization to retain the calls collected but did not pursue the request. The collection was purged from NSA databases No reports were issued.
(U) Section 704
(TS//SI//NF) There were violations of FAA Section 704 due to delays in detasking selectors when the targets were discovered to be in the United States, one violation for incorrect date ranges, and one violation for tasking a selector belonging to a U.S. person.
(U) Section 705b (b)(1) (b)(3)-P.L. 86-36
(TS//SI//NF) There were violations of FAA Section 705b due to detasking delays, one violation due to querying a selector when the target was in the United States, violations due to miscellaneous human error, one violation due to failure to follow procedure, one violation due to querying more data than authorized, one violation due to an unauthorized selector, and violations due to delays in purging data.

in response to a request from senior managers, an NSA	
analyst queried a raw SIGINT database using selectors associated with a U.S. person not	
authorized for collection under FAA. The analyst conducted the search because	
The analyst also believed that	
The analyst was	
before a U.S. person is targeted. The query produced no results and	no
reports were issued.	
(U) Other (b)(1) (b)(3)-P.L. 86-36	
(U) Unauthorized Access to SIGINT	
(S//REL TO USA, FVEY) There were incidents of unauthorized access to SIGINT, including FISA, FAA, and PAA data, due to procedural errors, sharing of accounts, human error, and lac of training.	
(U) Improper Storage of SIGINT Data	
(S//REL TO USA, FVEY) There were incidents of improper storage of SIGINT data, to include improperly labeled FISA data, U.S. identities entered into a database, and human error	
(U) Dissemination	
(S//REL TO USA, AUS, GBR, NZL) NSA terminated (b))(1))-P.L. 86-36)-50 USC 3024(i)
)-50 000 5024(1)
While researching the problem, NSA recognized and rectified weaknesses with additional oversight and internal controls related to filtering, training analysts and reviewing audit trails.	
(b)(3)-P.L. 86-36 (C//NF) data that was not releasable to	
e-mails were deleted upon recognition.	_1
(S//SI//REL TO USA, FVEY) By agreement, SIGINT intercept is forwarded.	1
notified	
NSA and destroyed the intercept. As a result of these instances, formal procedures for handlin U.S. person information are being developed for these	g
(TS//SI//NF) Computer Network Exploitation (CNE)	and the second
(b)(1) (b)(3)-P.L. 86-36 (b)(1)	
(b)(3)-50 USC 3024(i)	

CID: 4165174	TOP SEC	RET//COMINT//NOFORN	(b)(1) (b)(3)-P.L. 86-36 (b)(3)-18 USC 798 (b)(3)-50 USC 3024
(TS//SI//NF)			
	 		
			(b)(1)
	(U) Intellig	ence-related Activition	(b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(
(S//SI//NF) To re	duce the risk of unauth	orized telephony collection a	
instituted a proce	ss that gives analysts g	reater and faster insight into	a target's location
· · · ·			
collection occurre	ed, it was purged from	NSA's principal raw SIGINT	when required
		· · ·	
(TS//SI//NF) Sim	llarly.		
	NSA analysts	found that e-mail selector	ors
occurred in 0	of the instances was	1 P. T.	Collection that
		s purged from NSA database	(b)(3)-P.L. 86-36
(U/ /FOUO) Altho	ough not violations of F	E.O. 12333 and related direct	ives, the NSA reports 30-50 USC 30
instances in which	h database access was a cesses were terminated.	not terminated when it was no	o longer required. Once
identifica, the act	coses were terrimated.		
	litionally, there were	violations resulting from	collection on U.S. persons
as follows:	due to a	with data collected;	due to failure
to perform an on	gin check prior to tasking	due to	accessing a
database containi			and due to
,	sharing.		naturi il
		(b)(1)	
		(b)(3)-P.L. 86-36	

TOP SECRET//COMINT//NOFORN

	Studies		Special	
(U) Queries not Reviewed				
	(U// FOUO) Due to a lack of trained personn reviewing audit trails of raw SIGINT queries	s.		
		that account was subsequently susper	nded. NSA	
1	was not able to determine the volume of que		· ·	
	The site is arranging additional training.	ng for all site audit trail reviewers.		
	(U) Intelligence Oversight Inspections	S	(b)(1) (b)(3)-P.L. 86-36	
	(U) NSA/CSS Threat Operations Center	er (NTOC)		
	(U/FOUO) An NSA OIG inspection found to appropriately managed and compliant with remanagement controls to ensure that properly executed on the NTOC operations to inspection found a 95 percent rate of compliance.	regulations. NTOC has established effect auth floor. Based on training statistics review	tive porities are	
	(U) NSA/CSS Texas (NSAT)	tance for intemgence oversight training.	(b)(1) (b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i)	
	(U//FOUO) Joint IG inspectors examined in training, IO knowledge, and the application of NSAT operates well in the application of NS manager is well known and has begun to ma governing mission directive does not encome working NSAT missions or delineate Service highlight of the inspection was the meticulous within several mission product lines.	of IO. Despite fragmented oversight of ISA authorities. The recently appointed IGA improvements to the site's IO process apass responsibilities for the oversight of the Cryptologic Component (SCC) response	O training, O program ses. The reservists sibilities. A	
	(U// FOUO) Investigation of Alleged Im	enronriaties at NSA Georgia (NSAG	`	
b)(3)-P.L.		iproprieties at 143A deorgia (143Ad	,	
	(S//SI//REL TO USA, FVEY) On 14 Augus	at 2000, the NSA OIC completed an invest	stigation into	
		program at NSAG unlawfully intercepted		
	processed U.S. person communications.	program at 195AG umawitany intercept		
	processes C.B. person communications.			
		tion included four interviews of the comp	olainant,/	
	almost records. We for	and the forensic ana und no targeting of U.S. persons by	lysis of	
	(b)(1) (b)(3)-P.L. 86-36 TOP SECRET	I//COMINT//NOFORN 8	(b)(1) (b)(3)-P.L. 86-36 (b)(3)-50 USC 3024(i)	

TOP SECRET//COMINT//NOFORN

(U// FOUO)				/ (b)(3)-F.L. 00-30
há	ally, the NSA OIG substant ad queried a raw SIGINT of as a relative of a valid fore	ntiated an allegation that ar database on a selector of a eign intelligence target.	n NSAG analyst, person in the Unite	ed
(U// FOUO) Alleged of the United State	Unauthorized Discloses SIGINT System (US	ure of Classified Infor	mation and Misc	ise
queried an NSA datable auditor, the soldier comisuse, the soldier red Justice (UCMJ) Field Specialist, he was given	USSS to target his wife, who have for her confessed his actions. After ceived nonjudicial punishr. Grade Article 15, the sold ren 45 days extra duty, and ended for 180 days). In additional confession of the con	a soldier in a U.S. Army no was also a soldier station. Follow investigation by the unit sment. Through a Uniformatier's rank was reduced from the was required to forfeit didition, the unit has revoke	ving questions from substantiated the ed Code of Military m Sergeant to one half month's r	pay ess to (b)(1)
language. The	reportedly queried ording to the analyst, he que analyst's action was not	ueried the foreign numbers in support of his official, no classified information have	nission-related duti	the
P.L. 86-36			o o o o o o o o o o o o o o o o o o o	
(b (b	D)(1) D)(3)-P.L. 86-36 D)(3)-50 USC 3024(i)			